Pacific Journal of Mathematics

DIOPHANTINE DETERMINATIONS OF $3^{(p-1)/8}$ AND $5^{(p-1)/4}$

RICHARD HOWARD HUDSON

Vol. 111, No. 1 November 1984

DIOPHANTINE DETERMINATIONS OF $3^{(p-1)/8}$ AND $5^{(p-1)/4}$

RICHARD H. HUDSON

Let p be a prime =24f+1. The author and Kenneth S. Williams derived a criteria for 3 to be an eighth power (mod p) in terms of the parameters in the Diophantine systems a^2+b^2 and x^2+3y^2 . A new proof of this result is given which uses Jacobi sums. This proof is simpler in that it does not require summing 36 cyclotomic numbers; moreover, it leads simultaneously to new necessary and sufficient criteria for $3^{(p-1)/8}$ to be congruent to $b/a \pmod{p}$, $a \equiv 1 \pmod{4}$, b > 0. Using this result, criteria for $3^{(p-1)/8} \equiv 1$, b/a, -1, or $-b/a \pmod{p}$ are given in terms of the parameters in other well-known quadratic partitions of p or of 4p.

Let p be a prime = 20f + 1, $16p = x^2 + 50u^2 + 50v^2 + 125w^2$, $xw = v^2 - 4uv - u^2$. It is shown that $5^{(p-1)/4} \equiv 1 \pmod{p}$ if and only if $16 \mid w$ or $uv \equiv 2 \pmod{4}$. This result is of interest in relation to criteria given by Emma Lehmer for 2 to be a fifth power \pmod{p} and for p to be a hyperartiad.

1. Introduction and preliminaries. For a prime p = 24f + 1 we have the following quadratic partitions of p or of 4p:

(1)
$$p = a^2 + b^2$$
, $a \equiv 1 \pmod{4}$, (2) $p = c^2 + 2d^2$, $c \equiv 1 \pmod{4}$,

(3)
$$p = x^2 + 3y^2, x \equiv 1 \pmod{3}$$
, (4) $p = u^2 + 6v^2, u \equiv 1 \pmod{4}$,

(5)
$$4p = A^2 + 27B^2$$
, $A \equiv 1 \pmod{3}$.

Using the law of octic reciprocity given by A. E. Western [8], the value of $3^{(p-1)/8}$ has been given in terms of the Diophantine systems (1) and (2); specifically, we have

$$3^{(p-1)/8} \equiv 1 \pmod{p} \Leftrightarrow \begin{cases} a \equiv c \pmod{3} & \text{if } p \equiv 1 \pmod{48}, \\ a \equiv -c \pmod{3} & \text{if } p \equiv 25 \pmod{48}, \end{cases}$$

(b)

$$3^{(p-1)/8} \equiv b/a \pmod{p} \Leftrightarrow \begin{cases} b \equiv c \pmod{3} & \text{if } p \equiv 1 \pmod{48}, \\ b \equiv -c \pmod{3} & \text{if } p \equiv 25 \pmod{48}. \end{cases}$$

Throughout we fix b to be positive in case (b), as in [1, p. 3.7], by fixing a primitive root g(p) such that $g^{6f} \equiv b/a \pmod{p}$ for b > 0.

Using cyclotomic numbers of order 12 [9] and an index formula due to Muskat [7], Hudson and Williams [5] gave necessary and sufficient criteria for 3 to be an eighth power modulo p (case (a) above) in terms of the parameters in systems (1) and (3).

In this note we show that the Davenport-Hasse relation in a form given by Yamamoto [11] and certain relations between Jacobi sums of order 24 lead simultaneously to the result of Hudson and Williams [4] (and more neatly as the proof does not necessitate summing 36 cyclotomic numbers) and to a new criteria in case (b) (3 is not a fourth power (mod p)); see Theorem 1. Using this theorem, we obtain in this paper similar criteria in terms of parameters in (4) and (5), see Theorems 2 and 3. Finally, in (3.3) and Theorem 4, we delineate criteria for 5 to be a quartic residue (mod p = 20f + 1) in terms of the parameters in (3.1) in relation to Lehmer's [6] criteria for 2 to be a quintic residue.

As preliminaries, we require an easy modification of Wilson's theorem giving for a prime p = mnf + 1,

(1)
$$mf! nf! \equiv (-1)^{mf-1} \equiv (-1)^{nf-1} \pmod{p}.$$

Next, see, e.g. [5], for $1 \le s < r \le 23$, p = 24f + 1, we have

(1.2)
$${rf \choose sf} \equiv (-1)^{sf} {(24 - r + s)f \choose sf} \pmod{p}.$$

Finally, for a prime p = mnf + 1 we have from the Davenport-Hasse relation in the form given by Yamamoto [11, p. 488] that

(1.3)
$$(n^{(p-1)/m})^t \equiv \frac{ntf ! \prod_{j=1}^{n-1} (mjf)!}{\prod_{j=0}^{n-1} (mj + t)f!} \pmod{p}.$$

Our notation for Jacobi sums is as follows. Let χ_{24} be a character (mod p) of order 24, let $\phi_{24} = e^{2\pi i/24}$, and let g be a primitive root of p with $g^f \equiv \phi_{24} \pmod{\Omega}$ where Ω is a prime ideal divisor of p in $Q(\phi_{24})$. For $x \not\equiv 0 \pmod{p}$, let ind g(x) be the unique integer b such that $x \equiv g^b \pmod{p}$, $0 \le b \le p-2$. Then the Jacobi sum $J_{24}(r, s)$ of order 24 is defined by

$$J_{24}(r,s) = \sum_{x=0}^{p-1} \chi_{24}^{r}(x) \chi_{24}^{s}(1-x) = \sum_{x=2}^{p-1} \phi_{24}^{r \operatorname{ind}_{g}(x)+s \operatorname{ind}_{g}(1-x)}.$$

2. Diophantine determinations of $3^{(p-1)/8}$.

THEOREM 1. Let $p = 24f + 1 = a^2 + b^2 = x^2 + 3y^2$, $a \equiv 1 \pmod{4}$, b > 0. Then we have

(a)
$$3^{(p-1)/8} \equiv 1 \pmod{p} \Leftrightarrow \begin{cases} a \equiv 1 \pmod{3} & and \quad y \equiv 0 \pmod{8}, \\ a \equiv 2 \pmod{3} & and \quad y \equiv 4 \pmod{8}, \end{cases}$$

and

(b)
$$3^{(p-1)/8} \equiv b/a \pmod{p} \Leftrightarrow \begin{cases} b \equiv 1 \pmod{3} & and \quad y \equiv 0 \pmod{8} \\ b \equiv 2 \pmod{3} & and \quad y \equiv 4 \pmod{8}. \end{cases}$$

Proof. From [5, Th. 15.1] we have

(2.1)
$$\binom{8f}{2f} \equiv \begin{cases} +1 \text{ or } -1 \pmod{p} & \text{according as } a \equiv 1 \text{ or } 2 \pmod{3}, \\ b/a \text{ or } -b/a \pmod{p} & \text{according as } b \equiv 1 \text{ or } 2 \pmod{3}. \end{cases}$$

Moreover, it follows from Gauss [3] that

(2.2)
$${12f \choose 6f} \equiv 2a \pmod{p} \quad \text{for } a \equiv 1 \pmod{4}.$$

Using (1.1), (1.2), and (1.3) we have

$$2^{(p-1)/4} = (2^{(p-1)/12})^3 \equiv \frac{6f!12f!}{3f!15f!} \equiv \frac{\binom{18f}{3f}}{\binom{18f}{6f}} \equiv \frac{(-1)^f \binom{9f}{3f}}{\binom{12f}{6f}} \pmod{p},$$

$$3^{(p-1)/8} \equiv \frac{3f!8f!16f!}{f!9f!17f!} \equiv (-1)^f \frac{3f!7f!}{f!9f!} \equiv (-1)^f \frac{\binom{7f}{f}}{\binom{9f}{3f}},$$

from which it follows that

(2.3)
$$\frac{\binom{7f}{f}}{\binom{12f}{6f}} \equiv (-1)^{b/4} 3^{(p-1)/8} \pmod{p}.$$

From Berndt [1, pp. 3.17, 3.25, 3.23] we have

(2.4)
$$(-1)^{b/4+y/4} = (-1)^{v/2}$$
 and $J_{24}(1,7) = (-1)^{v/2}J_{24}(1,1)$.

Fixing a primitive root g(p) so that $g^{6f} \equiv b/a \pmod{p}$, b > 0, it follows from [10, Lemma 6] that

$$\binom{8f}{f} \equiv (-1)^{v/2} \binom{2f}{f} \equiv (-1)^{b/4 + y/4} \binom{2f}{f} \pmod{p}.$$

But clearly $\binom{8f}{f}\binom{7f}{f} = \binom{2f}{f}\binom{8f}{2f}$ so that, using (2.3),

$$3^{(p-1)/8} \equiv \frac{(-1)^{b/2+y/4} {8f \choose 2f}}{{12f \choose 6f}} \equiv \begin{cases} (-1)^{y/4} \pmod{p} \Leftrightarrow a \equiv 1 \pmod{3}, \\ (-1)^{y/4}b/a \pmod{p} \Leftrightarrow b \equiv 1 \pmod{3}. \end{cases}$$

This completes the proof of Theorem 1.

THEOREM 2. Let $p = 24f + 1 = a^2 + b^2 = u^2 + 6v^2$, $a \equiv 1 \pmod{4}$, b > 0. Then we have

(1)
$$3^{(p-1)/8} \equiv 1 \pmod{p} \Leftrightarrow \begin{cases} b \equiv 2v \pmod{8} & \text{and } a \equiv 1 \pmod{3}, \\ b \equiv -2v \pmod{8} & \text{and } a \equiv 2 \pmod{3}, \end{cases}$$

and

(2)
$$3^{(p-1)/8} \equiv b/a \pmod{p} \Leftrightarrow \begin{cases} b \equiv 2v \pmod{8} & and \ b \equiv 1 \pmod{3}, \\ b \equiv -2v \pmod{8} & and \ b \equiv 2 \pmod{3}. \end{cases}$$

Proof. Theorem 2 is an immediate consequence of Theorem 1 and the left-hand-side of (2.4).

THEOREM 3. Let $p = 24f + 1 = a^2 + b^2$, $a \equiv 1 \pmod{4}$ and b > 0, $4p = A^2 + 27B^2$ with $A \equiv 1 \pmod{2}$. Then we have

(a)
$$3^{(p-1)/8} \equiv 1 \pmod{p} \Leftrightarrow \begin{cases} B \equiv \pm 3 \pmod{8} & \text{and } a \equiv (-1)^f \pmod{3}, \\ B \equiv \pm 1 \pmod{8} & \text{and } a \equiv (-1)^{f+1} \pmod{3}, \end{cases}$$

(b)

$$3^{(p-1)/8} \equiv b/a \pmod{p} \Leftrightarrow \begin{cases} B \equiv \pm 3 \pmod{8} & \text{and } b \equiv (-1)^f \pmod{3}, \\ B \equiv \pm 1 \pmod{8} & \text{and } b \equiv (-1)^{f+1} \pmod{3}. \end{cases}$$

Proof. Not that $(-1)^f = +1 \Leftrightarrow x \equiv 1 \pmod{8}$ (and $(-1)^f = -1 \Leftrightarrow x \equiv 5 \pmod{8}$) as

(2.5)
$$x \equiv 1 \pmod{8} \Leftrightarrow x^2 + 3y^2 \equiv 1 \pmod{16}$$
.

It is easily seen that

(2.6)
$$B = \pm \frac{1}{3}(x - y) \quad \text{if } y \equiv 1 \pmod{3}, \\ B = \pm \frac{1}{3}(x + y) \quad \text{if } y \equiv 2 \pmod{3}.$$

Theorem 3 now follows from (2.5), (2.6), and Theorem 1.

THEOREM 4. Let $p = 24f + 1 = a^2 + b^2$, $a \equiv 1 \pmod{4}$ and b > 0, $4p = A^2 + 27B^2$ with $A \equiv 0 \pmod{2}$. Then we have

(a)
$$3^{(p-1)/8} \equiv 1 \pmod{p} \Leftrightarrow \begin{cases} B \equiv 0 \pmod{16} & and \ a \equiv 1 \pmod{3}, \\ B \equiv 8 \pmod{16} & and \ a \equiv 2 \pmod{3}, \end{cases}$$

(b)
$$3^{(p-1)/8} \equiv b/a \pmod{p} \Leftrightarrow \begin{cases} B \equiv 0 \pmod{16} & and b \equiv 1 \pmod{3}, \\ B \equiv 8 \pmod{16} & and b \equiv 2 \pmod{3}. \end{cases}$$

Proof. As $B = \pm 2y$ if $A \equiv 0 \pmod{2}$, we have $B \equiv 0 \pmod{16}$ if $y \equiv 0 \pmod{8}$ and $B \equiv 8 \pmod{16}$ if $y \equiv 4 \pmod{8}$ so that Theorem 4 follows from Theorem 1.

REMARK 1. Criteria (a) and (b) in Theorems 1 and 4 may be reformulated as

$$3^{(p-1)/8} \equiv (-1)^{y/4 + [a/3]} \pmod{p}$$
 if $3 \mid b$

and

$$3^{(p-1)/8} \equiv (-1)^{y/4+[b/3]+1}b/a \pmod{p}$$
 if $3 \mid a$,

and for A even $(\Leftrightarrow 2^{(p-1)/3} \equiv 1 \pmod{p})$ we have

$$3^{(p-1)/8} \equiv (-1)^{B/8 + [a/3]} \pmod{p}$$
 if $3 \mid b$

and

$$3^{(p-1)/8} \equiv (-1)^{B/8+[b/3]+1}b/a \pmod{p}$$
 if $3 \mid a$.

REMARK 2. Putting together the criteria in Theorem 1 and the criteria given at the beginning of this paper we see that the parameters c and y, $c \equiv 1 \pmod{4}$, are related for all primes $p = 24f + 1 = c^2 + 2d^2 = x^2 + 3y^2$ as follows:

$$y \equiv 0 \pmod{8} \Leftrightarrow c \equiv (-1)^f \pmod{3}$$
.

3. Criteria for 5 to be a fourth power (mod p). Let $p = 20f + 1 = a^2 + b^2 = e^2 + f^2$, $a \equiv e \equiv 1 \pmod{4}$;

(3.1)
$$16p = x^2 + 50u^2 + 50v^2 + 125w^2$$
, $x \equiv 1 \pmod{5}$, $xw = v^2 - 4uv - u^2$.

Gauss [3] showed that $5^{(p-1)/4} \equiv 1 \pmod{p} \Leftrightarrow 5 \mid b$. Recently it has been shown, see [2, p. 382], that $5^{(p-1)/4} \equiv 1 \pmod{p} \Leftrightarrow 2 \nmid e$, and that [4]

(3.2)
$$5^{(p-1)/4} \equiv 1 \pmod{p} \Leftrightarrow \begin{cases} x \equiv 4 \pmod{8}, \\ \text{or } \\ x \equiv \pm 2w \pmod{8}. \end{cases}$$

Using results of Emma Lehmer [6] we show that (3.2) can be reformulated as

(3.3)
$$5^{(p-1)/4} \equiv 1 \pmod{p} \Leftrightarrow 16 \mid w \text{ or } uv \equiv 2 \pmod{4}.$$

Embodied in (3.3) is considerably more information than in simpler criteria for 5 to be a fourth power (mod p) as is seen by the following theorem.

THEOREM 5. Let p = 20f + 1 be a prime satisfying (3.1). Then we have (a)

$$5^{(p-1)/4} \equiv 1 \pmod{p}$$
 and $2^{(p-1)/5} \equiv 1 \pmod{p} \Leftrightarrow 16 \mid w$,

(b)

$$5^{(p-1)/4} \equiv -1 \pmod{p}$$
 and $2^{(p-1)/5} \equiv 1 \pmod{p} \Leftrightarrow 16 \mid x$,

(c)

$$5^{(p-1)/4} \equiv 1 \pmod{p} \quad and \quad 2^{(p-1)/5} \not\equiv 1 \pmod{p} \Leftrightarrow uv \equiv 2 \pmod{4},$$

(d)

$$5^{(p-1)/4} \equiv -1 \pmod{p}$$
 and $2^{(p-1)/5} \not\equiv 1 \pmod{p} \Leftrightarrow 4 \mid uv;$

(e) in case (c),
$$2 \mid v \Leftrightarrow x \equiv 3w \pmod{8}$$
 and $2 \mid u \Leftrightarrow x \equiv -3w \pmod{8}$.

Proof. To prove \Rightarrow in (a) note that from [6, p. 13] we have x = 4a and w = 4d, $a \equiv -d \pmod{2}$, so that $8 \mid w$ in view of (3.2); moreover, $u \equiv v \equiv 0 \pmod{4}$, so that if $w \not\equiv 0 \pmod{16}$ we have, since $xw = v^2 - 4uv - u^2$, that $32 \equiv 16 - 0 - 16 \pmod{64}$, a clear impossibility. To prove \Leftarrow in (a) we have only to note that $16 \mid w \Rightarrow 2 \mid x$ and that $a \equiv -d \pmod{2} \Rightarrow x \equiv 4 \pmod{8}$. We omit the proof of (b) as it is entirely similar.

To prove (c) and (e) we note first that x odd and $x \equiv \pm 3w$ (mod 8) $\Leftrightarrow p - x^2 - 125w^2 \equiv 10 \pmod{16} \Leftrightarrow u^2 + v^2 \equiv 5 \pmod{8} \Leftrightarrow uv \equiv 2 \pmod{4}$, proving (c). Then (e) follows easily from $xw = v^2 - 4uv - u^2$. Finally (c) \Rightarrow (d) (u and v are of opposite parity as x is odd), completing the proof.

EXAMPLE. Let p = 101 so that (-29, 3, 2, 1) is a solution of (3.1). Since $uv \equiv 2 \pmod{4}$ and $2 \mid v$ we have $5^{(p-1)/4} \equiv 1 \pmod{p}$, $2^{(p-1)/5} \not\equiv 1 \pmod{p}$, and $x \equiv 3w \pmod{8}$.

REFERENCES

- [1] Bruce C. Berndt, Gauss and Jacobi sums, unpublished course notes, University of Illinois, Urbana, Illinois, 1978.
- [2] Bruce C. Berndt and Ronald J. Evans, Sums of Gauss, Jacobi, and Jacobsthal, J. Number Theory, 11 (1979), 349–398.
- [3] Carl Friedrich Gauss, *Theoria residuorum biquadraticorum*, Comment. I, Comment. Soc. Reg. Sci. Gottingensis rec., **6** (1828) (Werke, Göttingen, 1876).
- [4] Richard H. Hudson and Kenneth S. Williams, Some new residuacity criteria, Pacific J. Math., 91 (1980), 135-143.
- [5] _____, Binomial coefficients and Jacobi sums, to appear in Trans. Amer. Math. Soc.
- [6] Emma Lehmer, The quintic character of 2 and 3, Duke Math. J., 18 (1951), 11-18.
- [7] Joseph B. Muskat, On the solvability of $x^e \equiv e \pmod{p}$, Pacific J. Math., 14 (1964), 257–260.
- [8] A. E. Western, Some criteria for the residues of eighth and other powers, Proc. London Math. Soc., (2) 9 (1911), 244–272.
- [9] A. L. Whiteman, The cyclotomic numbers of order 12, Acta Arith. 6 (1960), 53-76.
- [10] _____, Theorems on Brewer and Jacobsthal sums. I, Proc. Sympos. Pure Math., 8 (1965), 44-55.
- [11] Koichi Yamamoto, On a conjecture of Hasse concerning multiplicative relations of Gaussian sums, J. Combinatorial Theory Ser. A, 1 (1966), 476–489.

Received December 9, 1981. Research supported by Natural Sciences and Engineering Research Council Canada grant A-7233.

University of South Carolina Columbia, SC 29208

PACIFIC JOURNAL OF MATHEMATICS EDITORS

DONALD BABBITT (Managing Editor)

University of California Los Angeles, CA 90024

Hugo Rossi University of Utah Salt Lake City, UT 84112

C. C. Moore and Arthur Ogus University of California Berkeley, CA 94720 J. Dugundji

Department of Mathematics University of Southern California Los Angeles, CA 90089-1113

R. FINN and H. SAMELSON

Stanford University Stanford, CA 94305

ASSOCIATE EDITORS

R. Arens E. F. Beckenbach

E. F. BECKENBACH (1906–1982) B. H. NEUMANN

F. Wolf

K. Yoshida

SUPPORTING INSTITUTIONS

UNIVERSITY OF ARIZONA
UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA, RENO
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY

UNIVERSITY OF OREGON
UNIVERSITY OF SOUTHERN CALIFORNIA
STANFORD UNIVERSITY
UNIVERSITY OF HAWAII
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON

Pacific Journal of Mathematics

Vol. 111, No. 1 November, 1984

Harald Brandenburg and Adam Stefan Mysior, For every Hausdorff	
space Y there exists a nontrivial Moore space on which all continuous	
functions into <i>Y</i> are constant	
Henry Dappa, A Marcinkiewicz criterion for L^p -multipliers	9
P. H. Doyle, III and John Gilbert Hocking, Bijectively related spaces. I.	
Manifolds	3
Joel Hass, Complete area minimizing minimal surfaces which are not totally	
geodesic 3	5
Aarno Hohti, On Ginsburg-Isbell derivatives and ranks of metric spaces 3	9
Richard Howard Hudson, Diophantine determinations of $3^{(p-1)/8}$ and	
$5^{(p-1)/4}$ 4	9
A. F. Izé and A. Ventura, Asymptotic behavior of a perturbed neutral	
functional-differential equation related to the solution of the unperturbed	
linear system5	7
Palle E. T. Jorgensen, Spectral representations of unbounded nonlinear	
operators on Hilbert space9	3
Darrell Conley Kent and Gary Douglas Richardson, Cauchy spaces with	
regular completions	
Mark Mahowald, An addendum to: "bo-resolutions"	7
Stuart Wayne Margolis and Jean-Eric Pin, Minimal noncommutative	
varieties and power varieties	5
Carla Massaza and Alfio Ragusa, Some conditions on the homology	
groups of the Koszul complex13	7
Vicente Miquel Molina, Some examples of Riemannian almost-product	
manifolds	3
Roderic Murufas, Inverse spectral problems for certain differential	
operators	9
Ulrich Oertel, Closed incompressible surfaces in complements of star	
links	9
Katsuro Sakai, A characterization of local equiconnectedness	1
William Victor Smith and Don Harrell Tucker, Weak integral	
convergence theorems and operator measures 24	3